Bemerkungen zum Hensel—Oreschen Hauptsatze.

Von MICHAEL BAUER in Budapest.

Es sei α eine primitive ganze Zahl des algebraischen Zahlkörpers $K = R(\alpha)$, welche der irreduziblen ganzzahligen Gleichung $F(x) = 0$ genügt. Die rationale Zahl p sei prim und es sei $F(x)$ (mod. p^ν) in irreduzible Faktoren, deren höchste Koeffizienten gleich Eins sind, zerlegt

(1) $$F(x) \equiv F_1(x) \ldots F_k(x) \ldots F_r(x) \qquad (\text{mod. } p^\nu).$$

Wir setzen voraus, daß $\nu \geqq \delta + 1$ ist, wo p^δ die höchste Potenz von p ist, die in der Diskriminante $D(F(x))$ enthalten ist. Im Körper K gilt

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_k^{e_k} \ldots \mathfrak{p}_r^{e_r},$$

wo $\mathfrak{p}_k$ ein Primideal g_k-ten Grades bedeutet. Gehört $\mathfrak{p}_k$ im Sinne von ORE[1]) zum Polynom $F_k(x)$, dann wird der Grad des Polynoms

(1*) $$n_k = e_k g_k,$$

wenn, wie vorausgesetzt, $\nu \geqq \delta + 1$ ausfällt.

Es seien p^{δ_k}, bzw. $p^{\varrho_{kl}}$, $(k \neq l)$ die höchsten Potenzen von p, welche in $D(F_k(x))$, bzw. in der Resultante $R(F_k(x), F_l(x))$ enthalten sind. Führen wir die Körper $K^{(k)} = R(\overline{\alpha}_k)$ ein, wo

$$F_k(\overline{\alpha}_k) = 0$$

ist und es sollen die Indexe der Zahlen α, bzw. $\overline{\alpha}_k$ bezüglich der Körper K, bzw. $K^{(k)}$ die höchsten Potenzen p^ψ, bzw. $p^{\overline{\psi}_k}$ enthalten. ORE[2]) bewies, daß, für genügend große ν, die Relation

[1]) Ö. ORE, Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, *Math. Annalen*, **96** (1927), S. 313—352, insb. S. 326.

[2]) A. a. O. [1]), S. 345 (Satz 6).

(2) $$\psi = \sum_{k=1}^{r} \overline{\psi}_k + \sum_{k>l} \varrho_{kl}$$

gilt, worin die Zahlen δ_k, $\overline{\psi}_k$, ϱ_{kl} invariant sind.

Es läßt sich beweisen, daß (2) schon für $\nu \geqq \delta + 1$ richtig ist. Bei jeder Zerlegung (1) sind im Falle $\nu \geqq \delta + 1$ die Zahlen δ_k, $\overline{\psi}_k$, ϱ_{kl} dieselben. Es treten noch andere invariante Zahlen auf.

1. Zunächst wird die Invarianz der Zahlen δ_k, ϱ_{kl} bewiesen. Ist $\nu \geqq \delta + 1$, dann besteht für zwei beliebige Zerlegungen von $F(x)$ (mod. p^ν) in irreduzible Faktoren, deren höchste Koeffizienten gleich Eins sind,

(3) $$\begin{aligned} F(x) &\equiv F_1(x) \ldots F_k(x) \ldots F_r(x) \pmod{p^\nu} \\ F(x) &\equiv G_1(x) \ldots G_k(x) \ldots G_r(x) \pmod{p^\nu}, \end{aligned}$$

nach ORE[3]) die Kongruenz

(3*) $$F_k(x) \equiv G_k(x) \pmod{p^{\nu-\delta}},$$

wenn die Polynome $F_k(x)$, $G_k(x)$ zum Primideal $\mathfrak{p}_k$ gehören. Aus der bekannten Relation

(4) $$\delta = \sum_{k=1}^{r} \delta_k + 2 \sum_{k>l} \varrho_{kl}$$

folgt, daß $D(F_k(x))$, $D(G_k(x))$ bzw. $R(F_k(x), F_l(x))$, $R(G_k(x), G_l(x))$ im Falle $\nu \geqq 2\delta + 1$ dieselben höchsten Potenzen von p enthalten. Jetzt läßt sich unsere Behauptung für $\nu \geqq \delta + 1$ beweisen. Ist nämlich

$$F(x) \equiv F_1(x) \ldots F_k(x) \ldots F_r(x) \pmod{p^\nu},$$

so kann man (mod. $p^{\nu+\mu}$) eine Zerlegung in irreduzible Faktoren, deren höchste Koeffizienten gleich Eins sind,

$$\begin{gathered} F(x) \equiv F_1^{(\mu)}(x) \ldots F_k^{(\mu)}(x) \ldots F_r^{(\mu)}(x) \pmod{p^{\nu+\mu}}, \\ \mu = 0, 1, 2, \ldots, \quad F_k^{(0)}(x) = F_k(x) \end{gathered}$$

angeben, wo

(1**) $$F_k^{(\mu)}(x) \equiv F_k(x) \pmod{p^{\nu-\varrho'}}, \quad \varrho' = \sum_{k>l} \varrho_k$$

ausfallen. Ist nun $\nu \geqq \delta + 1$, so wird

$$\nu - \varrho' \geqq \sum_{k=1}^{r} \delta_k + \varrho' + 1,$$

woraus unsere Behauptung folgt. (Hier haben wir die Theorie der p-adischen Zahlen bewußt vermieden.)

[3]) A. a. O. [1]), S. 332.

2. Komplizierter ist der Beweis der Invarianz der Zahlen $\overline{\psi}_k$. Wir werden die p-adischen Zahlen verwenden.[4]) Es sei in irreduzible p-adische Faktoren, deren höchste Koeffizienten gleich Eins sind, zerlegt

$$F(x) = P_1(x) \dots P_k(x) \dots P_r(x) \quad (p),$$

wo $P_k(x)$ der p-adische Grenzwert der Polynome $F_k^{(\mu)}(x)$ ist. Bezeichnen wir den Körper der rationalen p-adischen Zahlen durch P. Es ist am bequemsten (wenn auch nicht unbedingt notwendig) den Körper P zu einem solchen algebraisch abgeschlossenen Körper zu erweitern, welcher die gewöhnlichen algebraischen Zahlen enthält. Die gewöhnlichen Wurzeln von $F(x)$ liefern auch die p-adischen Wurzeln. Es seien die Wurzeln von $P_k(x)$

$$\beta_1^{(k)}, \dots, \beta_{n_k}^{(k)}.$$

Wenn die gewöhnlichen Wurzeln von $F_k(x) = 0$ gleich

$$\omega_1^{(k)}, \dots, \omega_{n_k}^{(k)}$$

sind (eine derselben ist $= \overline{\alpha}_k$), so sind bei geeigneter Bezeichnung im Falle $\nu \geqq \delta + 1$, die Körper

$$P(\beta_i^{(k)}) = P(\omega_i^{(k)}), \qquad (i = 1, 2, \dots, n_k).$$

In sämtlichen Körpern $P(\beta_i^{(k)})$, $R(\omega_i^{(k)})$ haben die Henselschen Primteiler, bzw. die Primideale, welche p teilen, denselben Grad g_k und die Multiplizität ist e_k. Die Diskriminanten der Körper (also auch die Diskriminante von $K^{(k)} = R(\overline{\alpha}_k)$) enthalten dieselbe höchste Potenz p^{d_k} von p. Da

$$\delta_k = 2\overline{\psi}_k + d_k \tag{5}$$

ausfällt, ist die Zahl $\overline{\psi}_k$ invariant für $\nu \geqq \delta + 1$.

---

[4]) Außer den grundlegenden Arbeiten von Hensel vgl. die Arbeit von K. Rychlík, Zur Bewertungstheorie der algebraischen Körper, *Journal für Math.*, **153** (1924), S. 94—107 und meine Noten: Die Theorie der p-adischen bzw. $\mathfrak{P}$-adischen Zahlen und die gewöhnlichen algebraischen Zahlkörper, *Math. Zeitschrift*, **14** (1922), S. 244—249 und **20** (1924), S. 95—97; Über die Erweiterung des Körpers der p-adischen Zahlen zu einem algebraisch abgeschlossenen Körper, *Math. Zeitschrift*, **19** (1924), S. 308—312; Über die Erweiterung eines algebraischen Zahlkörpers durch Henselsche Grenzwerte, *diese Acta*, **1** (1922—23), S. 74—79; Zur Theorie der algebraischen Körper, *diese Acta*, **2** (1924—26), S. 69–71. Wir erwähnen noch die große Abhandlung von A. Ostrowski, Untersuchungen zur arithmetischen Theorie der Körper, *Math Zeitschrift*, **39** (1935), S. 269—404.

Ist die höchste Potenz von p in der Diskriminante von K gleich p^d, so wird

$$\delta = 2\psi + d. \tag{5*}$$

Nach einem Satze von HENSEL ist

$$d = \sum_{k=1}^{r} d_k, \tag{6}$$

daraus folgt nach (4) die Richtigkeit der Relation (2).

3. Es sollen hier noch einige Bemerkungen folgen. Wenn man in Betracht zieht, daß die Zahlen δ_k, ϱ_{kl}, $\overline{\psi}_k$ für $\nu \geqq \delta + 1$ invariant sind, so sieht man, daß (2) für $\nu \geqq \delta + 1$ bewiesen ist, sobald dieselbe für genügend große ν feststeht. Wie schon erwähnt wurde, hat ORE[5]) gezeigt, daß (2) für genügend große ν richtig ist. In seinem Beweise wendet er die p-adischen Zahlen nicht an, aber er macht u. A. Gebrauch von seiner Zerlegung[6]) des Führers. Diese Theorie der Zerlegung kann hier beseitigt werden und so wird das Beweisverfahren vereinfacht. Das erreicht man, wenn die Relation (4) und

$$d_k = g_k h_k, \quad d = \sum_{k=1}^{r} g_k h_k \tag{7}$$

angewendet werden, worin die Zahl p^{d_k} für genügend große ν die höchste Potenz von p in der Diskriminante von $K^{(k)} = R(\overline{\alpha}_k)$[7]) und $\mathfrak{p}_k^{h_k}$, bzw. $\overline{\mathfrak{p}}_k^{h_k}$ die höchste Potenz von $\mathfrak{p}_k$, bzw. $\overline{\mathfrak{p}}_k$ in den Differenten der Körper K, bzw. $K^{(k)}$ ist. (Durch $\overline{\mathfrak{p}}_k$ bezeichnen wir das Primideal von $K^{(k)}$, welches p teilt, es ist $p = \overline{\mathfrak{p}}_k^{e_k}$.) Aus (7) folgt nach dem Punkte **2** die Relation (6).

Wir erwähnen noch, daß der von ORE bewiesene Satz 5 (S. 344) ebenfalls für $\nu \geqq \delta + 1$ richtig ist.

(Eingegangen am 9. Dezember 1935.)

---

[5]) A. a. O. [1]), S. 340—345.

[6]) A. a. O. [1]), S. 332—340.

[7]) Wir wissen, daß dies auch die höchste Potenz von p in der Diskriminante von $P(\beta_l^{(k)})$ ist. Die Zahl p^d ist die höchste Potenz von p in der Diskriminante von K.